

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :  
Yuusaku OHTA et al. :  
Serial No. NEW : **Attn: APPLICATION BRANCH**  
Filed August 28, 2003 : **Attorney Docket No. 2003\_1215A**  
**KEY DELIVERY APPARATUS, TERMINAL :  
APPARATUS, RECORDING MEDIUM,  
AND KEY DELIVERY SYSTEM :**

**CLAIM OF PRIORITY UNDER 35 USC 119**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

THE COMMISSIONER IS AUTHORIZED  
TO CHARGE ANY DEFICIENCY IN THE  
FEES FOR THIS PAPER TO DEPOSIT  
ACCOUNT NO. 23-0975

Sir:

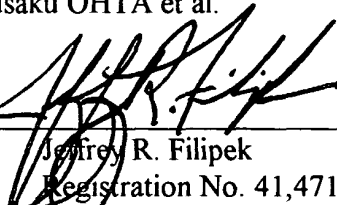
Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-249242, filed August 28, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Yuusaku OHTA et al.

By

  
\_\_\_\_\_  
Jeffrey R. Filipek  
Registration No. 41,471  
Attorney for Applicants

JRF/fs  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
August 28, 2003

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 8月28日

出 願 番 号

Application Number:

特願2002-249242

[ ST.10/C ]:

[ JP2002-249242 ]

出 願 人

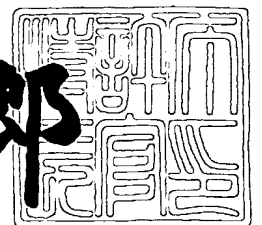
Applicant(s):

松下電器産業株式会社

2003年 6月 5日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3043715

【書類名】 特許願

【整理番号】 2022540328

【提出日】 平成14年 8月28日

【あて先】 特許庁長官 殿

【国際特許分類】 G11B 20/10  
G09C 1/00  
G06F 12/14

【発明者】

【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式  
会社内

【氏名】 太田 雄策

【発明者】

【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式  
会社内

【氏名】 山内 弘貴

【発明者】

【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式  
会社内

【氏名】 宮▲ざき▼ 雅也

【発明者】

【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式  
会社内

【氏名】 松崎 なつめ

【発明者】

【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式  
会社内

【氏名】 阿部 敏久

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003742

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】

情報利用鍵管理・配信装置及び情報利用端末及び記録媒体

【特許請求の範囲】

【請求項 1】 鍵情報を元に利用可能な情報の前記鍵情報を管理し、配信するためのネットワークに接続された装置であって、情報を利用するために必要な鍵情報を管理するための鍵情報管理手段と、鍵を配信する相手の正当性を判断するための認証手段と、前記鍵情報を配信する相手と通信するための通信手段とを含み、前記鍵情報を元に利用可能な情報を利用しようとする相手からの、鍵情報配信要求により、前記認証手段は前記通信手段を介して鍵情報配信要求相手の正当性を確認し、前記鍵情報管理手段は、前記認証手段により相手の正当性が確認されると、鍵情報配信の可否を判断し、鍵情報の配信を許可すると、前記通信手段を介して鍵情報を配信することを特徴とする情報利用鍵管理・配信装置。

【請求項 2】 鍵情報および前記鍵情報を元に利用可能な情報を利用するためのネットワークに接続された装置であって、情報利用鍵管理・配信装置から配信された前記鍵情報を格納するための鍵情報格納手段と、前記鍵情報を配信してもらう相手に、その正当性を証明するための認証手段と、前記鍵情報を配信してもらう相手と通信するための通信手段と、前記鍵情報を元に利用可能な情報を利用しているか否かを監視するための情報利用監視手段とを含み、前記通信手段を用いて、情報利用鍵管理・配信装置に前記鍵情報配信の要求を通知すると、前記情報利用鍵管理・配信装置からの、前記通信手段を介した認証要求により、前記認証手段は認証処理を行い、前記情報利用鍵管理・配信装置から前記鍵情報配信の正当性が認められ、かつ前記鍵情報の配信が許可された場合に、配信された前記鍵情報を前記鍵情報格納手段に格納し、自身の保有する鍵情報を元に利用可能な情報を利用し、前記情報の利用は前記情報利用監視手段により監視されており、前記情報利用監視手段が前記情報の利用終了を検出すると、前記鍵情報格納手段は鍵情報を消去し、前記通信手段を用いて鍵情報消去の旨を前記情報利用鍵管理・配信装置に通知することを特徴とする情報利用端末。

【請求項 3】 鍵情報および前記鍵情報を元に利用可能な情報を利用するため

の記録媒体であって、情報利用鍵管理・配信装置から配信された前記鍵情報を格納するための鍵情報格納手段と、前記鍵情報を配信してもらう相手に、その正当性を証明するための認証手段とを含み、前記鍵情報格納手段および前記認証手段は、情報利用鍵管理・配信装置に接続され、前記情報利用鍵管理・配信装置からの鍵情報配信処理により、前記認証手段は前記情報利用鍵管理・配信装置の認証手段と認証処理を行い、前記情報利用鍵管理・配信装置から前記鍵情報配信の正当性が認められ、かつ前記鍵情報の配信が許可された場合に、配信された前記鍵情報を前記鍵情報格納手段に格納し、自身の保有する鍵情報を元に利用可能な情報を利用することを特徴とする記録媒体。

【請求項 4】 鍵情報格納手段および認証手段は情報利用端末の通信手段に接続され、前記情報利用端末の前記通信手段を介して、情報利用鍵管理・配信装置から鍵情報を配信されることを特徴とする請求項 2 記載の記録媒体。

【請求項 5】 鍵情報管理手段は鍵情報を元に利用可能な情報毎の鍵情報の総数を管理する請求項 1 記載の情報利用鍵管理・配信装置。

【請求項 6】 鍵情報管理手段として、日付や時間を管理するための時間管理手段を含む請求項 1 または請求項 5 記載の情報利用鍵管理・配信装置。

【請求項 7】 鍵情報格納手段として、日付や時間を管理するための時間管理手段を含む請求項 2 記載の情報利用端末。

【請求項 8】 時間管理手段に設定された日時に、情報利用鍵管理・配信装置の鍵情報管理手段で管理されている鍵情報の個数が更新され、情報利用端末の鍵格納手段に格納されている鍵が消去される請求項 6 記載の情報利用鍵管理・配信装置。

【請求項 9】 時間管理手段に設定された日時に、情報利用鍵管理・配信装置から、特定の情報利用端末へ鍵情報が配信される請求項 6 記載の情報利用鍵管理・配信装置。

【請求項 10】 通信手段として、特定の鍵情報を元に利用可能な情報の鍵情報を保有している情報利用端末を特定するために、各端末に前記鍵情報有無を問い合わせることが可能な請求項 1 または請求項 5 または請求項 7 または請求項 8 または請求項 9 記載の情報利用鍵管理・配信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、例えば、情報の複製を制限して著作権の保護を図る情報管理方法を用いた情報利用鍵管理・配信装置、情報利用端末、記録媒体に関する。

【0002】

【従来の技術】

従来、例えばエス・ディー・エム・アイ（SDMI；Secure Digital Music Initiative）における著作権の保護が必要な音楽情報に対しては、該情報の複製に関する管理が行われてきた。具体的には、情報の無制限な複製を防止するために複製の回数を有限にすることや、複製の複製（以下「孫コピー」と呼ぶことがある）の許可・禁止を管理するための複製の世代管理に関する制限などがそれにあたる。

【0003】

【発明が解決しようとする課題】

ところで、上記のような複製の管理は、主にパーソナルコンピュータ（以下「PC」と呼ぶことがある）や専用レコーダなどの記録装置と、SDカードのような半導体型記録媒体やDVDのような光ディスクなどの記録媒体との間で行われるが、このような複製管理方式の元では、図14に示されるように、例えば、ある記録装置1401から記録媒体1402あるいは1403に複製した複製制限付情報1410を、別の記録装置1404に複製することはできなかった。これは、複製に関する管理情報を、コピー元である記録装置1401が一元管理していることに起因するが、ユーザの利便性という観点からは自由度が低く、必ずしも好ましいものではなかった。

【0004】

そこで、本発明は上記事情を考慮してなされたもので、ネットワークに接続された情報利用鍵管理・配信装置と情報利用端末間で、複製に関する制限が設けられた情報を、その制限の範囲内で著作権を保護しつつ自由に複製するための、情報利用鍵管理・配信装置および情報利用端末を提供することを目的とする。

また、本発明は、情報利用鍵管理・配信装置から記録媒体に、複製に関する制限が設けられた情報を、その制限の範囲内で著作権を保護しつつ自由に複製するための、記録媒体を提供することを目的とする。

【 0 0 0 5 】

また、本発明は、情報利用鍵管理・配信装置から情報利用端末に接続された記録媒体に、複製に関する制限が設けられた情報を、その制限の範囲内で著作権を保護しつつ自由に複製するための、記録媒体を提供することを目的とする。

また、本発明は、複製に関する制限として時間に関する制限を管理することが可能で、かつその制限の範囲内で著作権を保護しつつ自由に複製するための、情報複製管理ネットワークシステムを提供することを目的とする。

【 0 0 0 6 】

また、本発明は、情報利用端末のうち、どの情報利用端末が鍵情報を保有しているかを知ることが可能な情報利用鍵管理・配信装置、情報利用端末、記録媒体を提供することを目的とする。

本発明は、情報の複製範囲を有限にすることにより、著作権の保護を実現する情報管理に特に有効である。

【 0 0 0 7 】

【課題を解決するための手段】

本発明の請求項 1 記載の発明は、鍵情報を元に利用可能な情報の前記鍵情報を管理し、配信するためのネットワークに接続された装置であって、情報を利用するために必要な鍵情報を管理するための鍵情報管理手段と、鍵を配信する相手の正当性を判断するための認証手段と、前記鍵情報を配信する相手と通信するための通信手段とを含み、前記鍵情報を元に利用可能な情報を利用しようとする相手からの、鍵情報配信要求により、前記認証手段は前記通信手段を介して鍵情報配信要求相手の正当性を確認し、前記鍵情報管理手段は、前記認証手段により相手の正当性が確認されると、鍵情報配信の可否を判断し、鍵情報の配信を許可すると、前記通信手段を介して鍵情報を配信することを特徴とする情報利用鍵管理・配信装置であり、認証処理によりその正当性が認められた情報利用相手は、複製に関する制限が設けられた情報を自由に複製することができ、かつ認証処理によ



りその正当性が認められなかった情報利用相手は情報の利用が制限されることになり、著作権の保護を実現しつつ、自由度の高い複製が行える、という作用を有する。

## 【 0 0 0 8 】

本発明の請求項 2 記載の発明は、鍵情報および前記鍵情報を元に利用可能な情報を利用するためのネットワークに接続された装置であって、情報利用鍵管理・配信装置から配信された前記鍵情報を格納するための鍵情報格納手段と、前記鍵情報を配信してもらう相手に、その正当性を証明するための認証手段と、前記鍵情報を配信してもらう相手と通信するための通信手段とを含み、前記通信手段を用いて、情報利用鍵管理・配信装置に前記鍵情報配信の要求を通知すると、前記情報利用鍵管理・配信装置からの、前記通信手段を介した認証要求により、前記認証手段は認証処理を行い、前記情報利用鍵管理・配信装置から前記鍵情報配信の正当性が認められ、かつ前記鍵情報の配信が許可された場合に、配信された前記鍵情報を前記鍵情報格納手段に格納し、自身の保有する鍵情報を元に利用可能な情報を利用することを特徴とする情報利用端末であり、認証処理によりその正当性が認められた情報利用端末は、複製に関する制限が設けられた情報を自由に複製することができ、かつ認証処理によりその正当性が認められなかった情報利用端末は情報の利用が制限されることになり、著作権の保護を実現しつつ、自由度の高い複製が行える、という作用を有する。

## 【 0 0 0 9 】

本発明の請求項 3 記載の発明は、鍵情報および前記鍵情報を元に利用可能な情報を利用するための記録媒体であって、情報利用鍵管理・配信装置から配信された前記鍵情報を格納するための鍵情報格納手段と、を含み、前記鍵情報格納手段および前記認証手段は、情報利用鍵管理・配信装置に接続され、前記情報利用鍵管理・配信装置からの鍵情報配信処理により、前記認証手段は前記情報利用鍵管理・配信装置の認証手段と認証処理を行い、前記情報利用鍵管理・配信装置から前記鍵情報配信の正当性が認められ、かつ前記鍵情報の配信が許可された場合に、配信された前記鍵情報を前記鍵情報格納手段に格納し、自身の保有する鍵情報を元に利用可能な情報を利用することを特徴とする記録媒体であり、認証処理に

よりその正当性が認められた記録媒体は、複製に関する制限が設けられた情報を自由に複製することができ、かつ認証処理によりその正当性が認められなかった記録媒体は情報の利用が制限されることになり、著作権の保護を実現しつつ、自由度の高い複製が行える、という作用を有する。

## 【 0 0 1 0 】

本発明の請求項 4 記載の発明は、鍵情報格納手段および認証手段は情報利用端末の通信手段に接続され、前記情報利用端末の前記通信手段を介して、情報利用鍵管理・配信装置から鍵情報を配信されることを特徴とする請求項 2 記載の記録媒体であり、記録媒体は必ずしも情報利用鍵管理・配信装置に直接接続する必要はなく、情報利用端末の通信手段を介して鍵情報の配信を受けることが可能であり、著作権の保護を実現しつつ、自由度の高い情報の利用が可能になる、という作用を有する。

## 【 0 0 1 1 】

本発明の請求項 5 記載の発明は、鍵情報管理手段は鍵情報を元に利用可能な情報毎の鍵情報の総数を管理する請求項 1 記載の情報利用鍵管理・配信装置であり、鍵情報として鍵情報の総数を管理し、同時に利用できる情報の数を制限することが可能になる、という作用を有する。

本発明の請求項 6 記載の発明は、鍵情報管理手段として、日付や時間を管理するための時間管理手段を含む請求項 1 または請求項 5 記載の情報利用鍵管理・配信装置であり、時間に基づいた鍵情報の管理が可能になる、という作用を有する。

## 【 0 0 1 2 】

本発明の請求項 7 記載の発明は、鍵情報格納手段として、日付や時間を管理するための時間管理手段を含む請求項 2 記載の情報利用端末であり、時間に基づいた鍵情報の取り扱いが可能になる、という作用を有する。

本発明の請求項 8 記載の発明は、時間管理手段に設定された日時に、情報利用鍵管理・配信装置の鍵情報管理手段で管理されている鍵情報の個数が更新され、情報利用端末の鍵格納手段に格納されている鍵が消去される請求項 6 記載の情報利用鍵管理・配信装置および請求項 7 記載の情報利用端末であり、情報利用端

末では、設定時間により、自動的に鍵情報利用できなくなる、という作用を有する。

【 0 0 1 3 】

本発明の請求項 9 記載の発明は、時間管理手段に設定された日時に、情報利用鍵管理・配信装置から、特定の情報利用端末へ鍵情報が配信される請求項 6 記載の情報利用鍵管理・配信装置であり、鍵情報配信時間の予約が可能になる、という作用を有する。

本発明の請求項 1 0 記載の発明は、通信手段として、特定の鍵情報を元に利用可能な情報の鍵情報を保有している情報利用端末を特定するために、各端末に前記鍵情報有無を問い合わせることが可能な請求項 1 または請求項 5 または請求項 7 または請求項 8 または請求項 9 記載の情報利用鍵管理・配信装置であり、鍵情報を保有する端末を通信手段により管理できる、という作用を有する。

【 0 0 1 4 】

【発明の実施の形態】

以下、本発明の実施の形態について、図 1 から図 1 3 を用いて詳細に説明する。

(第 1 の実施の形態)

図 1 に本発明の第 1 の実施の形態に係るネットワークシステムの構成図を示す。図 1 は、情報利用鍵管理・配信装置 0 1 0 1 と、端末 0 1 1 1、0 1 1 2、0 1 1 3、0 1 1 4、0 1 1 5 からなるネットワークで、通信プロトコルとしては例えばアイピー（IP；インターネットプロトコル）プロトコルが使用される。図 1 を用いて、まず「メンバ」、「非メンバ」、「グループ」の言葉を定義する。

【 0 0 1 5 】

「メンバ」は認証手段をもち、かつ情報利用鍵管理・配信装置 0 1 0 1 と同じ共通秘密情報を有する情報利用端末 0 1 1 1、0 1 1 2 を指す。

「非メンバ」は認証手段を持たない情報利用端末 0 1 1 4 や認証手段は持つが共通秘密情報を持たない端末 0 1 1 3 を指す。

「グループ」は情報利用鍵管理・配信装置 0 1 0 1 および「メンバ」情報利用

端末 0 1 1 1、0 1 1 2 を要素とする集合の名称である。

ここで、共通秘密情報は例えば情報利用鍵管理・配信装置 0 1 0 1 から配布される。このように「メンバ」を要素とする集合「グループ」を定義し、「非メンバ」と区別することにより、複製の範囲を有限なものとして明確に定義することが可能となり、情報の無制限な複製およびグループ外への流出を防止することができる。

#### 【 0 0 1 6 】

情報利用端末を「メンバ」と「非メンバ」に区別した場合、鍵情報の配信について次の 2 種類の組み合わせがあることが分かる。すなわち、情報利用鍵管理・配信装置 0 1 0 1 から「メンバ」情報利用端末への鍵情報配信と、情報利用鍵管理・配信装置 0 1 0 1 から「非メンバ」情報利用端末への鍵情報配信である。

。以下に、それぞれの組み合わせの場合の鍵配信手順についてに説明する。説明をより具体的にするため、以下の説明では鍵管理情報として、鍵情報を元に利用可能な情報の情報識別番号を C 1 として、情報識別番号 C 1 と、情報識別番号 C 1 に対応した鍵情報 K 1 および鍵情報配信可能総数 N 1 の 3 種類の情報を元に話を進める。図 2 は前述の鍵管理情報の概念図である。

#### 【 0 0 1 7 】

なお、本実施の形態では鍵情報を元に利用可能な情報自体の複製は、情報利用鍵管理・配信装置からメンバ情報利用端末、およびメンバ情報利用端末とメンバ情報利用端末の間では無制限に行うことが可能であるとする。

ただし、情報利用鍵管理・配信装置から非メンバ情報利用端末への情報の複製は禁止されるか、あるいは、情報利用鍵管理・配信装置が管理する鍵情報配信可能数を上限として、複製可能であるとしてもよい。なおこの場合は、情報利用鍵管理・配信装置から非メンバ情報利用端末への情報の複製が行われる度に、鍵情報配信可能数の上限は 1 ずつ減じられるものとする。

#### 【 0 0 1 8 】

また、メンバ情報利用端末から非メンバ情報利用端末への、鍵情報を元に利用可能な情報の複製は禁止されている。

またなお、この鍵情報を元に利用可能な情報は、その全てが暗号化されており

、その暗号情報を復号化するために、情報利用鍵管理・配信装置から鍵情報を配信してもらうものとする。ただし、必ずしも全てが暗号化されておらず、その一部が暗号化されている情報もあってよい。

#### ＜情報利用鍵管理・配信装置からメンバ情報利用端末への鍵情報配信＞

図 3 は本発明の第 1 の実施の形態に係る、情報利用鍵管理・配信装置 0 3 1 0 が管理する鍵情報を情報利用端末 0 3 2 0 に配信するための、それぞれの構成要素を図式化したものである。図 3 において、0 3 1 1 は鍵情報を管理するための鍵情報管理手段であり、0 3 1 2 および 0 3 2 2 は鍵情報配信の正当性を確認するための認証手段であり、0 3 1 3 および 0 3 2 3 は、互いが通信するための通信手段であり、0 3 2 4 は利用するために鍵情報が必要な情報の利用の有無を監視するための情報利用監視手段であり、0 3 2 5 は利用するために鍵情報が必要な情報である。

#### 【0 0 1 9】

また図 4 は、情報利用鍵管理・配信装置 0 3 1 0 が管理する鍵情報を情報利用端末 0 3 2 0 に配信する際のフローチャート図である。

以下に図 3 および図 4 を用いて、情報利用鍵管理・配信装置 0 3 1 0 から、情報利用端末 0 3 2 0 への鍵配信の手順を詳細に説明する。

図 3 に示されるように、情報利用端末 0 3 2 0 はあらかじめ利用するために鍵情報が必要な情報 0 3 2 5 を保有しており、情報利用端末の利用者の操作などにより、情報利用鍵管理・配信装置 0 3 1 0 への鍵情報配信要求が通信手段 0 3 2 3 を介して送信される（図 4 の 0 4 2 1）と、情報利用鍵管理・配信装置 0 3 1 0 は配信要求を受信し（図 4 の 0 4 1 1）、認証手段 0 3 1 2 および 0 3 2 2 は、通信手段 0 3 1 3 および 0 3 2 3 を介して、互いの間で認証処理を開始（図 4 の 0 4 1 2 および 0 4 2 2）する。認証の方法としては、例えば、ゼロ知識証明を利用したチャレンジアンドレスポンス型のハンドシェイクが利用される。

#### 【0 0 2 0】

認証処理の結果、情報利用端末 0 3 2 0 の鍵配信の正当性が確認されると、情報利用鍵管理・配信装置 0 3 1 0 の鍵情報管理手段 0 3 1 1 は配信要求された鍵情報の利用可能数がゼロでないことを確認（図 4 の 0 4 1 3）し、次の手順へ進

む。あるいは、この時配信要求された鍵情報の利用可能数がゼロの場合は、配信不可能なため、配信不完遂として、処理を完了する（図4の0417および0430）。なお、この鍵情報管理手段0311が管理する情報は、秘匿領域に格納されており、通常のアクセスはできないようにされているのが望ましい。

鍵情報管理手段0311は、鍵情報が配信可能であると判断すると、通信手段0313および0323を介して情報利用端末0320に鍵情報を配信する（図4の0414）。なお、このとき配信される鍵情報は、前述のチャレンジアドレスポンス型のハンドシェイク時に生成された一時的な暗号鍵により、暗号化されて配信されるのが望ましい。

#### 【0021】

情報利用端末0320は配信された鍵情報を受信すると（図4の0423）、鍵情報を鍵情報格納手段0321に格納し（図4の0424）、情報利用監視手段0324は情報利用の監視を開始する。なお、この監視は、鍵情報の配信により完了され、他の情報利用が開始されるまでか、あるいは情報利用端末の利用が電氣的に終了されるまでとする。なお、この鍵情報格納手段0321は秘匿領域に格納されており、通常のアクセスはできないようにされているのが望ましい。

#### 【0022】

情報利用鍵管理・配信装置0310は鍵情報の配信後、鍵情報管理手段0311の鍵情報配信可能数を「-1」し、更新する（図4の0415）。

情報利用監視手段0324が情報利用端末0320の情報利用終了を検出すると（図4の0427）、鍵情報可能手段0321内の鍵情報を消去し（図4の0428）、通信手段0323を介してその旨を情報利用鍵管理・配信装置0310に通知する（図4の0429）。

#### 【0023】

情報利用鍵管理・配信装置0310は該通知を受信すると、鍵情報管理手段0311に管理されている鍵情報配信可能数を「+1」し元に戻す。

なお、図4の0412および0422の認証処理の結果、メンバであることの正当性が証明できなかったときには、鍵情報の配信を拒否し、配信不完遂として処理を終了する（図4の0417および0430）。

## 【 0 0 2 4 】

上記で述べたように本発明の第 1 の実施の形態では、利用するために鍵情報が必要な情報を利用する際に、認証手段を有する端末をネットワークで接続することにより、「メンバ」端末と「非メンバ」端末の区別が可能となり、複製の範囲を有限なものにとどめることが可能となり、また、鍵情報配信に関して、配信可能数を有限にすることにより著作権を保護しつつ、グループ内での自由な複製が可能となる。

## (第 2 の実施の形態)

図 5 に本発明の第 2 の実施の形態に係るネットワークシステムの構成図を示す。図 5 は、情報利用鍵管理・配信装置 0 5 0 1 と、端末 0 5 1 1、0 5 1 2、0 5 1 3、0 5 1 4 からなるネットワークと、記録媒体 0 5 1 5、0 5 1 6、0 5 1 7、0 5 1 8 からなる。図 5 を用いて、記録媒体に関する「メンバ」、「非メンバ」、「グループ」の言葉を定義する。

## 【 0 0 2 5 】

「メンバ」記録媒体は認証手段をもち、かつ情報利用鍵管理・配信装置 0 5 0 1 と同じ共通秘密情報を有する記録媒体 0 5 1 5、0 5 1 6 を指す。

「非メンバ」記録媒体は認証手段を持たない記録媒体 0 5 1 7 や認証手段は持つが共通秘密情報を持たない記録媒体 0 5 1 6 を指す。

「グループ」は情報利用鍵管理・配信装置 0 5 0 1 および「メンバ」情報利用端末 0 5 1 1、0 5 1 2 を要素とする集合の名称である。

ここで、共通秘密情報は例えば情報利用鍵管理・配信装置 0 5 0 1 から配布される。このように「メンバ」、「非メンバ」、「グループ」の言葉の定義を記憶媒体に対して拡張することにより、端末への複製に限定されることなく、記憶媒体への複製を含めて、複製の範囲を有限なものとして明確に定義することが可能となり、情報の無制限な複製およびグループ外への流出を防止することができる。

## 【 0 0 2 6 】

記録媒体を「メンバ」と「非メンバ」に区別した場合、情報利用鍵管理・配信装置と記録媒体の間の鍵情報の配信について、次の 2 種類の組み合わせがあることが分かる。すなわち、情報利用鍵管理・配信装置 0 5 0 1 から「メンバ」記録

媒体 0 5 1 5 や 0 5 1 6 への鍵情報配信と、情報利用鍵管理・配信装置 0 5 0 1 から「非メンバ」記録媒体 0 5 1 7 や 0 5 1 8 への鍵情報配信である。

【 0 0 2 7 】

以下に、それぞれの組み合わせの場合の鍵配信手順についてに説明する。鍵管理情報としては第 1 の実施の形態と同情報を元に説明する。

なお、本実施の形態では鍵情報を元に利用可能な情報自体の複製は、情報利用鍵管理・配信装置からメンバ記録媒体およびメンバ情報利用端末からメンバ記録媒体の間では無制限に行うことが可能であるとする。

【 0 0 2 8 】

ただし、情報利用鍵管理・配信装置から非メンバ記録媒体への情報の複製は禁止されるか、あるいは、情報利用鍵管理・配信装置が管理する鍵情報配信可能数を上限として、複製可能であるとしてもよい。なおこの場合は、情報利用鍵管理・配信装置から非メンバ記録媒体への情報の複製が行われる度に、鍵情報配信可能数の上限は 1 ずつ減じられるものとする。

【 0 0 2 9 】

また、メンバ情報利用端末から非メンバ記録媒体への、鍵情報を元に利用可能な情報の複製は禁止されている。

またなお、この鍵情報を元に利用可能な情報は、その全てが暗号化されており、その暗号情報を復号化するために、情報利用鍵管理・配信装置から鍵情報を配信してもらうものとする。

ただし、必ずしも全てが暗号化されておらず、その一部が暗号化されている情報もあってよい。

< 情報利用鍵管理・配信装置からメンバ記録媒体への鍵情報配信 >

図 6 は本発明の第 2 の実施の形態に係る、情報利用鍵管理・配信装置 0 6 1 0 が管理する鍵情報を記録媒体 0 6 2 0 に配信するための、それぞれの構成要素を図式化したものである。図 6 において、0 6 1 1 は鍵情報を管理するための鍵情報管理手段であり、0 6 1 2 および 0 6 2 2 は鍵情報配信の正当性を確認するための認証手段であり、0 6 2 1 は配信された鍵情報を格納するための鍵情報格納手段であり、0 6 1 3 は、通信するための通信手段であり、0 6 2 3 は利用する



ために鍵情報が必要な情報である。

#### 【 0 0 3 0 】

また図 7 は、情報利用鍵管理・配信装置 0 6 1 0 が管理する鍵情報を記録媒体 0 6 2 0 に配信する際のフローチャート図である。

以下に図 6 および図 7 を用いて、情報利用鍵管理・配信装置 0 6 1 0 から、記録媒体 0 6 2 0 への鍵配信の手順を詳細に説明する。

図 6 に示されるように、記録媒体 0 6 2 0 はあらかじめ利用するために鍵情報が必要な情報 0 6 2 3 を保有しており、記録媒体 0 6 2 0 の利用者の操作などにより、情報利用鍵管理・配信装置 0 6 1 0 へ図 6 のように接続され、鍵配信処理を開始すると（図 7 の 0 7 2 1）、記録媒体 0 6 2 0 は配信要求を受信し（図 7 の 0 7 2 1）、認証手段 0 6 1 2 および 0 6 2 2 は互いの間で認証処理を開始（図 7 の 0 7 1 2 および 0 7 2 2）する。認証の方法としては、例えば、第 1 の実施の形態で述べた方法が利用される。

#### 【 0 0 3 1 】

認証処理の結果、記録媒体 0 6 2 0 の鍵配信の正当性が確認されると、情報利用鍵管理・配信装置 0 6 1 0 の鍵情報管理手段 0 6 1 1 は配信要求された鍵情報の利用可能数がゼロでないことを確認（図 7 の 0 7 1 3）し、次の手順へ進む。あるいは、この時配信要求された鍵情報の利用可能数がゼロの場合は、配信不可能なため、配信不完遂として、処理を完了する（図 7 の 0 7 1 7 および 0 7 3 0）。なお、この鍵情報管理手段 0 6 1 1 が管理する情報は、秘匿領域に格納されており、通常のアクセスはできないようにされているのが望ましい。

#### 【 0 0 3 2 】

鍵情報管理手段 0 6 1 1 は、鍵情報が配信可能であると判断すると、記録媒体 0 6 2 0 に鍵情報を配信する（図 7 の 0 7 1 4）。

なお、このとき配信される鍵情報は、前述のチャレンジアンドレスポンス型のハンドシェイク時に生成された一時的な暗号鍵により、暗号化されて配信されるのが望ましい。

#### 【 0 0 3 3 】

記録媒体 0 6 2 0 は配信された鍵情報を受信すると（図 7 の 0 7 2 3）、鍵情

報を鍵情報格納手段 0 6 2 1 に格納（図 7 の 0 7 2 4）する。なお、この鍵情報格納手段 0 6 2 1 は秘匿領域に格納されており、通常のアクセスはできないようにされているのが望ましい。

情報利用鍵管理・配信装置 0 6 1 0 は鍵情報の配信後、鍵情報管理手段 0 6 1 1 の鍵情報配信可能数を「- 1」し、更新する（図 7 の 0 7 1 5）。

#### 【 0 0 3 4 】

なお、鍵情報格納手段 0 6 2 1 内の鍵情報の消去および鍵情報管理手段 0 6 1 1 内の鍵情報の「+ 1」処理については第 3 の実施の形態で詳しく述べる。

またなお、図 7 の 0 4 1 2 および 0 4 2 2 の認証処理の結果、メンバであることの正当性が証明できなかったときには、鍵情報の配信を拒否し、配信不完遂として処理を終了する（図 7 の 0 4 1 7 および 0 4 3 0）。

#### 【 0 0 3 5 】

上記で述べたように、記録媒体を「メンバ」と「非メンバ」に区別することにより、本発明の第 1 の実施の形態で述べた効果に加え、情報利用鍵管理・配信装置 0 6 1 0 と記録媒体 0 6 2 0 の間での利用するために鍵情報が必要な情報の利用について、著作権の保護を実現しつつ、自由な複製が可能となる。

#### （第 3 の実施の形態）

図 8 は本発明の第 3 の実施の形態に係る、情報利用鍵管理・配信装置 0 8 1 0 が管理する鍵情報を、情報利用端末 0 8 2 3 に接続された記録媒体 0 8 2 3 0 に配信するための、それぞれの構成要素を図式化したものである。図 8 において、0 8 1 1 は鍵情報を管理するための鍵情報管理手段であり、0 8 1 2 および 0 8 2 2 および 0 8 3 2 は鍵情報配信の正当性を確認するための認証手段であり、0 8 2 1 および 0 8 3 1 は配信された鍵情報を格納するための鍵情報格納手段であり、0 8 1 3 および 0 8 2 3 は、通信するための通信手段であり、0 8 3 3 は利用するために鍵情報が必要な情報である。

#### 【 0 0 3 6 】

また図 9 は、情報利用鍵管理・配信装置 0 8 1 0 が管理する鍵情報を記録媒体 0 8 3 0 に配信する際のフローチャート図である。

以下に図 8 および図 9 を用いて、情報利用鍵管理・配信装置 0 8 1 0 から、記

録媒体 0 8 3 0 への鍵配信の手順を詳細に説明する。

図 8 に示されるように、記録媒体 0 8 2 0 はあらかじめ利用するために鍵情報が必要な情報 0 8 3 3 を保有しており、記録媒体 0 8 3 0 の利用者の操作などにより、情報利用端末 0 8 2 0 へ図 8 のように接続され、鍵配信要求を送信すると（図 9 の 0 9 2 1 ）、鍵情報管理・配信装置 0 8 1 0 は配信要求を受信し（図 9 の 0 9 1 1 ）、認証手段 0 8 1 2 および 0 8 3 2 は、通信手段 0 8 1 3 および 0 8 2 3 を介し、互いの間で認証処理を開始（図 9 の 0 9 1 2 および 0 9 2 2 ）する。認証の方法としては、例えば、第 1 の実施の形態で述べた方法が利用される。

#### 【 0 0 3 7 】

認証処理の結果、記録媒体 0 8 3 0 の鍵配信の正当性が確認されると、情報利用鍵管理・配信装置 0 8 1 0 の鍵情報管理手段 0 8 1 1 は配信要求された鍵情報の利用可能数がゼロでないことを確認（図 9 の 0 9 1 3 ）し、次の手順へ進むあるいは、この時配信要求された鍵情報の利用可能数がゼロの場合は、配信不可能なため、配信不完遂として、処理を完了する（図 9 の 0 9 1 7 および 0 9 3 0 ）。なお、この鍵情報管理手段 0 8 1 1 が管理する情報は、秘匿領域に格納されており、通常のアクセスはできないようにされているのが望ましい。鍵情報管理手段 0 8 1 1 は、鍵情報が配信可能であると判断すると、通信手段 0 8 1 3 および 0 8 2 3 を介し、記録媒体 0 8 3 0 に鍵情報を配信する（図 9 の 0 9 1 4 ）。なお、このとき配信される鍵情報は、前述のチャレンジアンドレスポンス型のハンドシェイク時に生成された一時的な暗号鍵により、暗号化されて配信されるのが望ましい。

#### 【 0 0 3 8 】

記録媒体 0 8 3 0 は配信された鍵情報を受信すると（図 9 の 0 9 2 3 ）、鍵情報を鍵情報格納手段 0 8 3 1 に格納し（図 9 の 0 9 2 4 ）、情報利用端末の情報利用監視手段 0 8 2 4 は情報利用の監視を開始する。なお、この監視は、鍵情報の配信により完了され、他の情報利用が開始されるまでか、あるいは情報利用端末の利用が電氣的に終了されるまでとする。なお、この鍵情報格納手段 0 8 3 1 は秘匿領域に格納されており、通常のアクセスはできないようにされているのが

望ましい。

【 0 0 3 9 】

情報利用鍵管理・配信装置 0 8 1 0 は鍵情報の配信後、鍵情報管理手段 0 8 1 1 の鍵情報配信可能数を「- 1」し、更新する（図 9 の 0 9 1 5）。

情報利用監視手段 0 8 2 4 が情報利用端末 0 8 2 0 の情報利用終了を検出すると（図 9 の 0 9 2 7）、鍵情報可能手段 0 8 3 1 内の鍵情報を消去し（図 9 の 0 9 2 8）、通信手段 0 8 2 3 を介してその旨を情報利用鍵管理・配信装置 0 8 1 0 に通知する（図 9 の 0 9 2 9）。

【 0 0 4 0 】

情報利用鍵管理・配信装置 0 8 1 0 は該通知を受信すると、鍵情報管理手段 0 8 1 1 に管理されている鍵情報配信可能数を「+ 1」し元に戻す。

なお、図 9 の 0 9 1 2 および 0 9 2 2 の認証処理の結果、メンバであることの正当性が証明できなかったときには、鍵情報の配信を拒否し、配信不完遂として処理を終了する（図 9 の 0 9 1 7 および 0 9 3 0）。

【 0 0 4 1 】

上記で述べたように、記録媒体を情報利用端末に接続した場合についても、情報利用端末の通信手段を介して鍵情報の配信を行うことにより、本発明の第 2 の実施の形態で述べた効果と同等の効果が得られる。

（第 4 の実施の形態）

図 1 0 および図 1 1 は本発明の第 4 の実施の形態に係る、鍵情報管理手段 1 0 0 1 と鍵情報格納手段 1 1 0 1 の各構成要素を図式化したものである。

【 0 0 4 2 】

図 1 0 では、鍵情報管理手段 1 0 0 1 内に、現在の鍵情報配信可能総数  $N_1$ 、 $N_2$  と設定時間  $T_1$ 、 $T_2$  と設定時間後の鍵情報の総数  $n_1$ 、 $n_2$  とがそれぞれ設定された鍵情報 1 0 2 1、1 0 2 2 が管理されており、特に設定時間について、時間管理手段 1 0 1 0 が管理している。

また、図 1 1 では、鍵情報格納手段 1 1 0 1 内に、現在の鍵情報配信可能総数  $M_1$ 、 $M_2$  と設定時間  $T_1$ 、 $T_2$  と設定時間後の鍵情報の総数  $m_1$ 、 $m_2$  とがそれぞれ設定された鍵情報 1 1 2 1、1 1 2 2 が格納されており、特に設定時間に

について、時間管理手段 1 1 1 0 が管理している。なお図 1 1 の鍵情報格納手段 1 1 0 1 は、情報利用端末のそれであってもよいし、記録媒体のそれであってもよい。

【 0 0 4 3 】

鍵情報 1 1 2 1、1 1 2 2 内の設定時間 T 1、T 2 は、第 1 の実施の形態から第 3 の実施の形態で述べた鍵情報配信時に、鍵情報とともに配信される。

なお、設定時間情報は、鍵情報と同様、一時的な暗号鍵により、暗号化されて配信されるのが望ましい。

また、鍵情報管理手段 1 0 0 1、鍵情報格納手段 1 1 0 1 は、秘匿領域であり、通常のアクセスはできないようにされているのが望ましい。

【 0 0 4 4 】

以下に、図 1 0 および図 1 1 を用いて、設定時間情報を含む鍵情報 1 0 2 1、1 0 2 2、1 1 2 1、1 1 2 2 に基づく鍵管理方法の手順を具体的に説明する。

鍵情報格納手段 1 1 0 1 において、時間管理手段 1 1 1 0 は、鍵情報 1 1 2 1 や 1 1 2 2 内の設定時間情報と同じ時間を自身で管理し、設定時間 T 1 と同時刻になると、鍵情報格納手段 1 1 0 1 内の鍵情報 1 1 2 1 を消去し、その旨を情報利用鍵管理・配信装置に通知する。また、設定時間 T 2 と同時刻になると、鍵情報格納手段 1 1 0 1 内の鍵情報 1 1 2 2 を消去し、その旨を情報利用鍵管理・配信装置に通知する。なお、鍵情報格納手段 1 1 0 1 は、時間管理手段 1 1 1 0 を持たない場合でも、情報利用鍵管理・配信装置からの鍵情報消去通知を受けると鍵情報を消去する、としてもよい。

【 0 0 4 5 】

鍵情報管理手段 1 0 0 1 において、時間管理手段 1 0 1 0 は、鍵情報 1 0 2 1 や 1 0 2 2 内の設定時間情報と同じ時間を自身で管理し、設定時間 T 1 と同時刻になると、鍵情報 1 0 2 1 の鍵情報配信可能総数 N 1 を「+ 1」する。また、設定時間 T 2 と同時刻になると、鍵情報 1 0 2 2 の鍵情報配信可能総数 N 2 を「+ 1」する。なお、鍵情報管理手段 1 0 0 1 は、時間管理手段 1 0 1 0 を持たない場合でも、情報利用端末からの鍵情報消去通知を受けると、鍵情報配信可能総数を「+ 1」できるとしてもよい。また、同時刻に複数の情報利用端末が鍵情報を

消去する場合は、その端末の台数分だけ、鍵情報配信可能総数を増やすことができることは言うまでもない。

#### 【 0 0 4 6 】

上記で述べたように、鍵情報管理手段 1 0 0 1 や鍵情報格納手段 1 1 0 1 に時間管理手段 1 0 1 0、1 1 1 0 を設けることにより、第 1 の実施の形態から第 3 の実施の形態で述べた効果に加え、情報利用監視手段を用いる方法とは別の方法として、時間による鍵情報の消去や更新が可能となる。

(第 5 の実施の形態)

図 1 2 は、本発明の第 5 の実施の形態に係る、鍵情報管理手段 1 2 0 1 の各構成要素を図式化したものである。

#### 【 0 0 4 7 】

図 1 2 では、鍵情報管理手段 1 2 0 1 内に、現在の鍵情報配信可能総数  $N_1$ 、 $N_2$  と設定時間  $T_1$ 、 $T_2$  と設定時間後の鍵情報の総数  $n_1$ 、 $n_2$ 、鍵情報配信先端末  $P_1$ 、 $P_2$  とがそれぞれ設定された鍵情報 1 2 2 1、1 2 2 2 が管理されており、特に設定時間について、時間管理手段 1 2 1 0 が管理している。なお、鍵情報管理手段 1 2 0 1 は秘匿領域であり、通常のアクセスはできないようにされているのが望ましい。

#### 【 0 0 4 8 】

以下に、図 1 2 を用いて、設定時間情報を含む鍵情報 1 2 2 1、1 2 2 2、1 2 7 1、1 2 7 2 に基づく鍵管理方法の手順を具体的に説明する。

鍵情報管理手段 1 2 0 1 が管理する鍵情報に設定時間情報  $T_1$ 、 $T_2$  と鍵情報配信先端末  $P_1$ 、 $P_2$  が設定されている場合、時間管理手段 1 2 1 0 は設定時間  $T_1$ 、 $T_2$  と同じ時刻を自身で管理しており、設定された時刻がくると、指定された鍵情報配信先端末  $P_1$  や  $P_2$  との間で、第 1 の実施の形態から第 3 の実施の形態で述べたような鍵情報配信処理を自動的に開始する。なお、設定時間と鍵情報配信先端末は必ずしも 1 対 1 に設定されている必要はなく、例えば一つの設定時刻に複数の情報利用端末に配信するような設定があってもよい。この場合、鍵情報の総数は配信した端末の台数分減じられることは言うまでもない。

#### 【 0 0 4 9 】

上記で述べたように、鍵情報管理手段 1 2 0 1 に時間管理手段 1 2 1 0 を設けることにより、第 1 の実施の形態から第 3 の実施の形態で述べた効果に加え、設定時間による自動的な鍵情報の配信が可能となる。

(第 6 の実施の形態)

図 1 3 は、本発明の第 6 の実施の形態に係る、ある特定の鍵情報を保有する情報利用端末を検索したい情報利用鍵管理・配信装置 1 3 0 1 と、検索対照の鍵情報を保有する情報利用端末 1 3 0 2、接続された記録媒体が検索対象情報を保有する情報利用端末 1 3 0 3、検索対象の情報を保有しない情報利用端末 1 3 0 4 間での鍵情報検索時の模式図である。

【0 0 5 0】

以下に図 1 3 を用いて、検索したい鍵情報を検索するときの手順を具体的に説明する。

まず情報を検索したい情報利用鍵管理・配信装置 1 3 0 1 は、自身と同一グループに属するメンバ情報利用端末 1 3 0 2、1 3 0 3、1 3 0 4 へ、同報通信的な方法を用いて、検索したい情報の情報識別番号を送信する(図 1 3 の矢印 1 3 1 1、1 3 1 2、1 3 1 3)。

【0 0 5 1】

各情報利用端末の鍵情報格納手段および各情報利用端末に接続された記録媒体は、自身が保有する鍵情報を管理しており、受信した検索中の鍵情報の情報識別番号と、自身が管理する情報識別番号とを比較し、同一の情報がある場合には、送信元の端末 1 3 0 1 に該情報を保有している旨を返信する(図 1 3 の矢印 1 3 2 1、1 3 2 2)。

【0 0 5 2】

上記のように本発明の第 6 の実施の形態では、通信手段として、検索したい鍵情報を同報通信的に問い合わせ、検索したい鍵情報を保有する情報利用端末を特定する手段を設けることにより、本発明の第 1 の実施の形態から第 5 の実施の形態で述べた効果に加え、鍵情報を配信した端末を自身のデータベースなどで管理せずに、検索したい鍵情報を保有する情報利用端末を管理することが可能となる。

【 0 0 5 3 】

(その他の変形例)

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

(1) 上記の各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。

【 0 0 5 4 】

(2) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blue-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【 0 0 5 5 】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。



【 0 0 5 6 】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(3) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【 0 0 5 7 】

【発明の効果】

以上のように、本発明によれば、請求項 1 から請求項 3 に従って、情報利用鍵管理・配信装置、情報利用端末、記録媒体の間での、情報の複製自体は有限の範囲内で無制限に行える代わりに、情報を利用するためには鍵情報が必要で、その鍵情報の配信を有限にすることにより、著作権の保護を実現しつつ、複製する側が複製に関する情報を一元管理していた従来技術と比べ、より自由度の高い情報の複製が可能になる、という効果が得られる。

【 0 0 5 8 】

また、請求項 6 に係る発明によれば、鍵情報の管理に時間管理手段を設けることにより、時間に基づいた鍵情報の管理が可能になる、という効果が得られる。

また、請求項 1 0 に係る発明によれば、通信手段として、鍵情報保有情報利用端末を問い合わせ、特定する手段を設けることにより、通信手段を用いて、ある特定の鍵情報を保有する情報利用端末の管理が可能になる、という効果が得られる。

【図面の簡単な説明】

【図 1】

ネットワーク端末における「メンバ」、「非メンバ」、「グループ」の概念図

【図 2】

鍵情報の概念図

【図 3】

情報利用鍵管理・配信装置から情報利用端末へ鍵情報を配信するための構成図

【図 4】

情報利用鍵管理・配信装置から情報利用端末へ鍵情報を配信する際のフローチャート

【図 5】

端末・記録媒体に関する「メンバ」、「非メンバ」、「グループ」の概念図

【図 6】

情報利用鍵管理・配信装置から記録媒体へ鍵情報を配信するための構成図

【図 7】

情報利用鍵管理・配信装置から記録媒体へ鍵情報を配信する際のフローチャート

【図 8】

情報利用鍵管理・配信装置から情報利用端末に接続された記録媒体へ鍵情報を配信するための構成図

【図 9】

情報利用鍵管理・配信装置から情報利用端末に接続された記録媒体へ鍵情報を配信するためのフローチャート

【図 1 0】

鍵情報管理手段が時間管理手段を含むときの鍵情報との関係を示した模式図

【図 1 1】

鍵情報格納手段が時間管理手段を含むときの鍵情報との関係を示した模式図

【図 1 2】

設定時間後に鍵情報配信処理が実行される鍵情報を管理するための鍵情報管理手段の構成図

【図 1 3】

情報利用鍵管理・配信装置が検索したい鍵情報を検索する際の、通信に関する模式図

【図 1 4】

従来の複製制限付情報の複製方法の概念図

【符号の説明】

0 3 1 0 情報利用鍵管理・配信装置

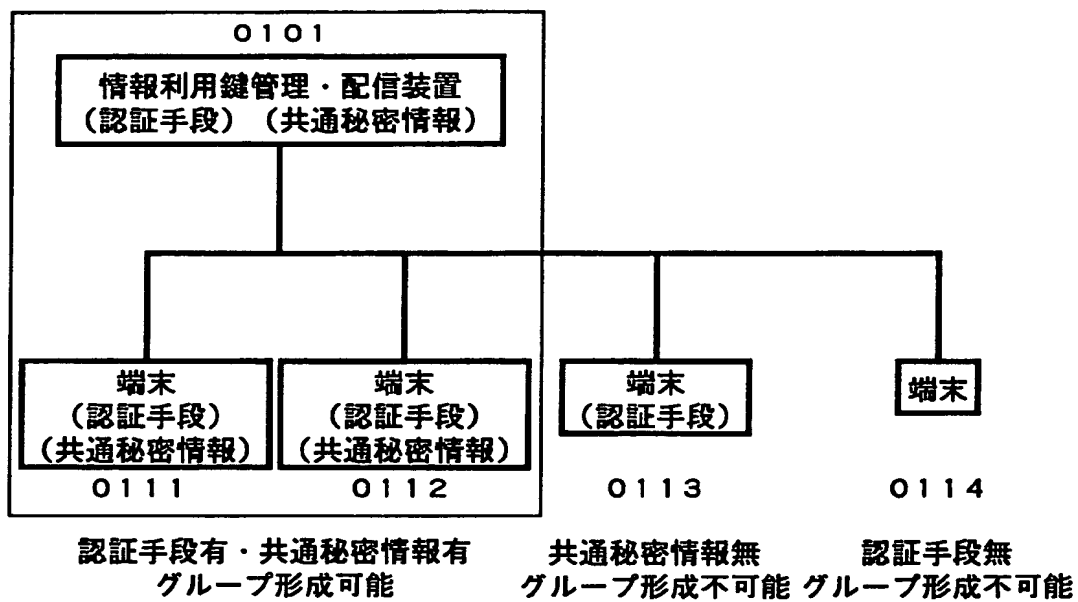
0 3 1 1 鍵情報管理手段

0 3 1 2 認証手段

0 3 1 3 通信手段

【書類名】 図面

【図 1】



【図 2】

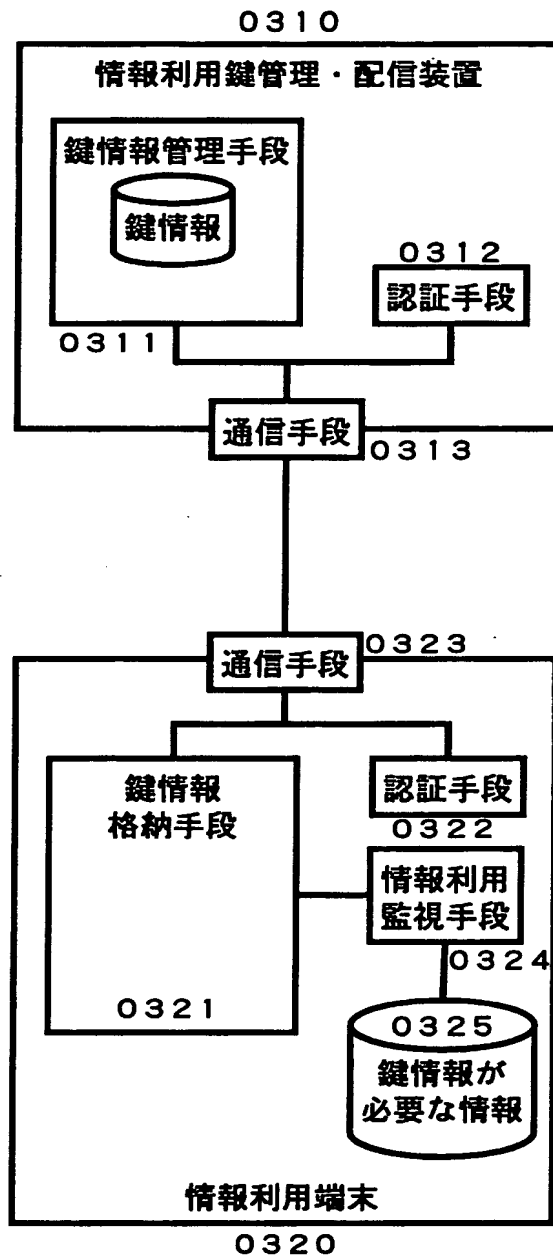
0201

情報識別番号：C 1  
鍵情報：K 1  
鍵情報総数：N 1

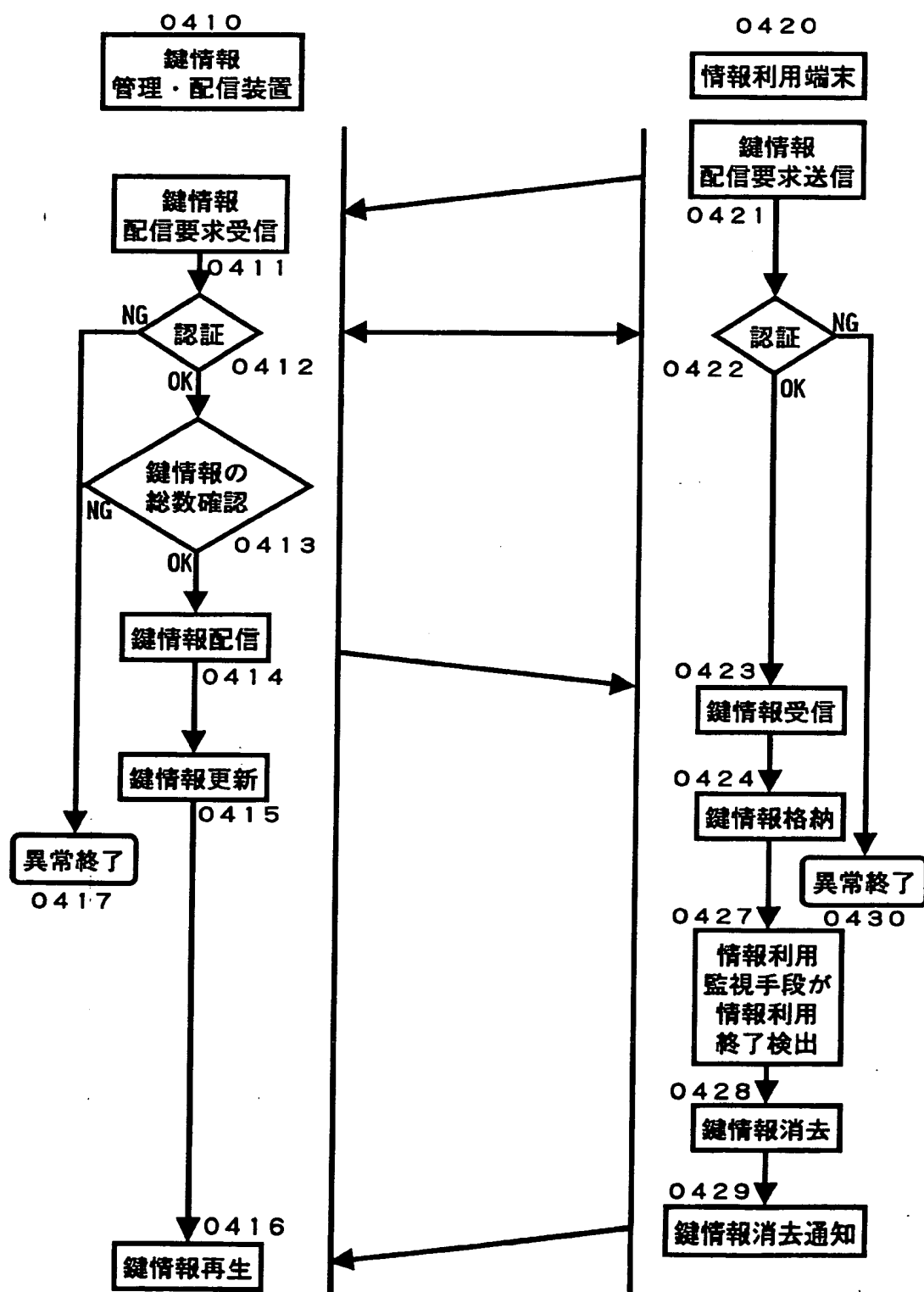
利用時に鍵情報が  
必要な情報  
情報識別番号：C 1

0211

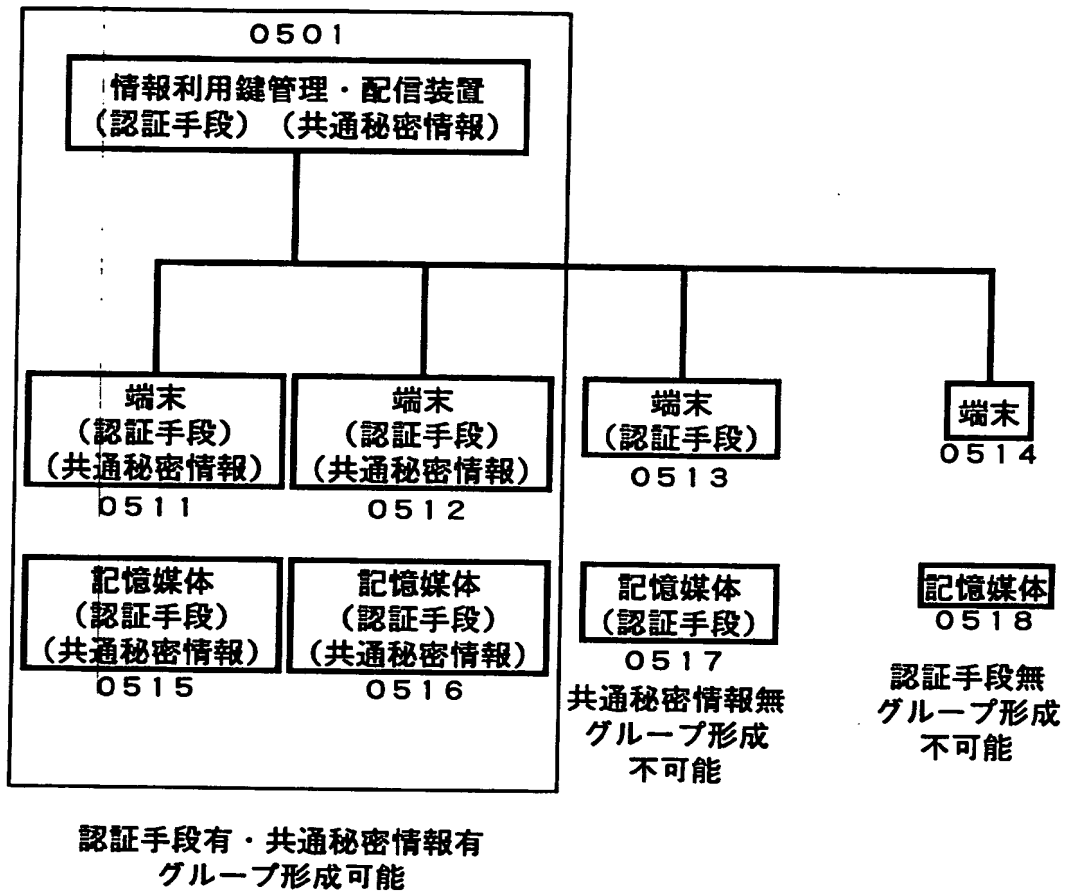
【図 3】



【図4】

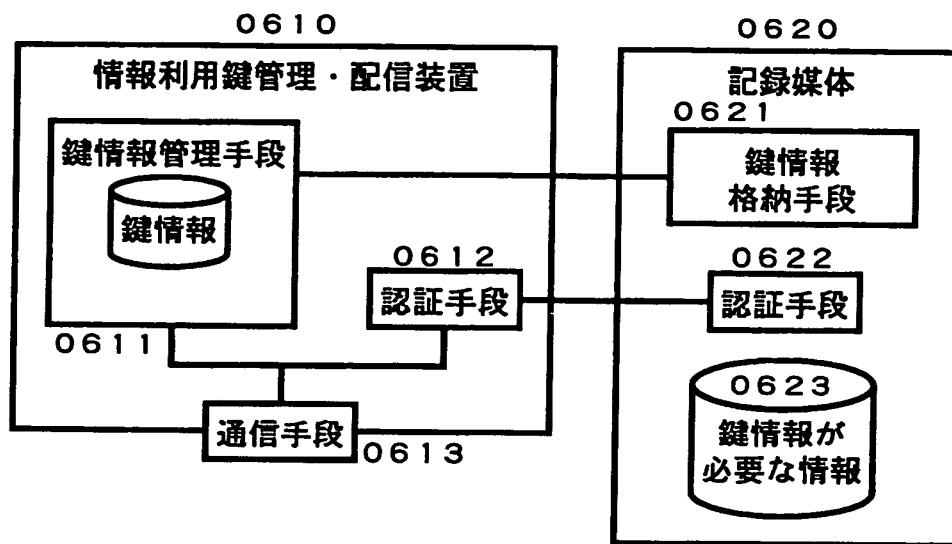


【図 5】

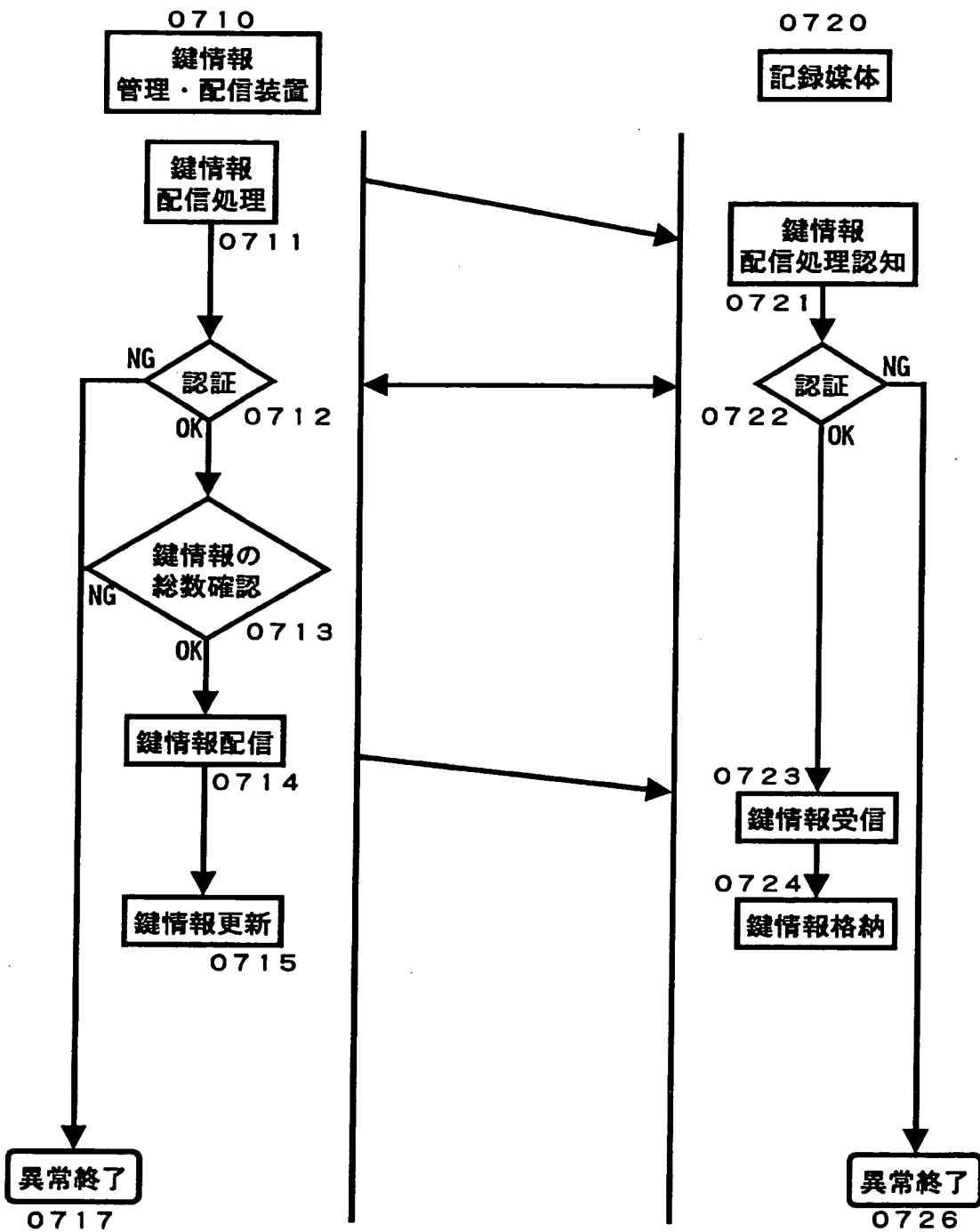




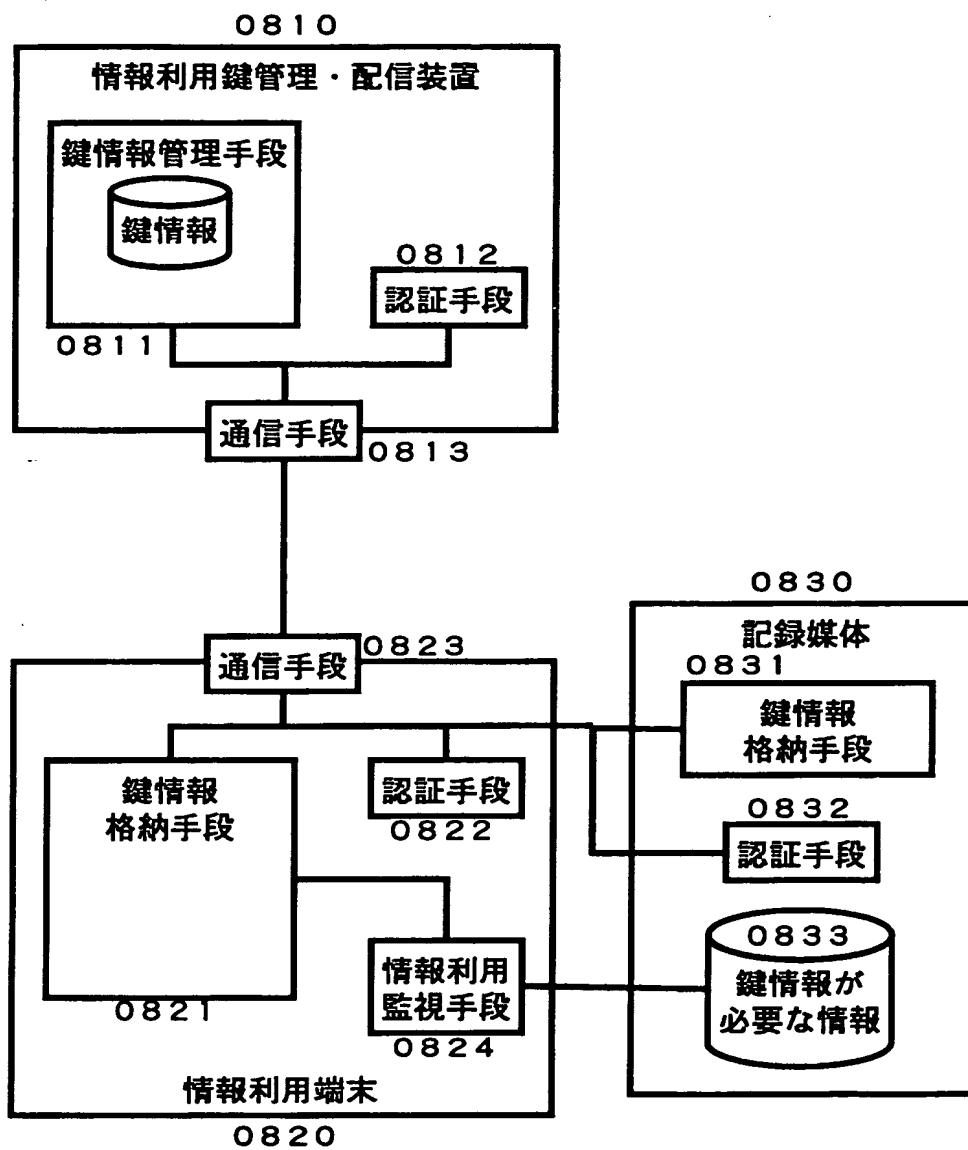
【図6】



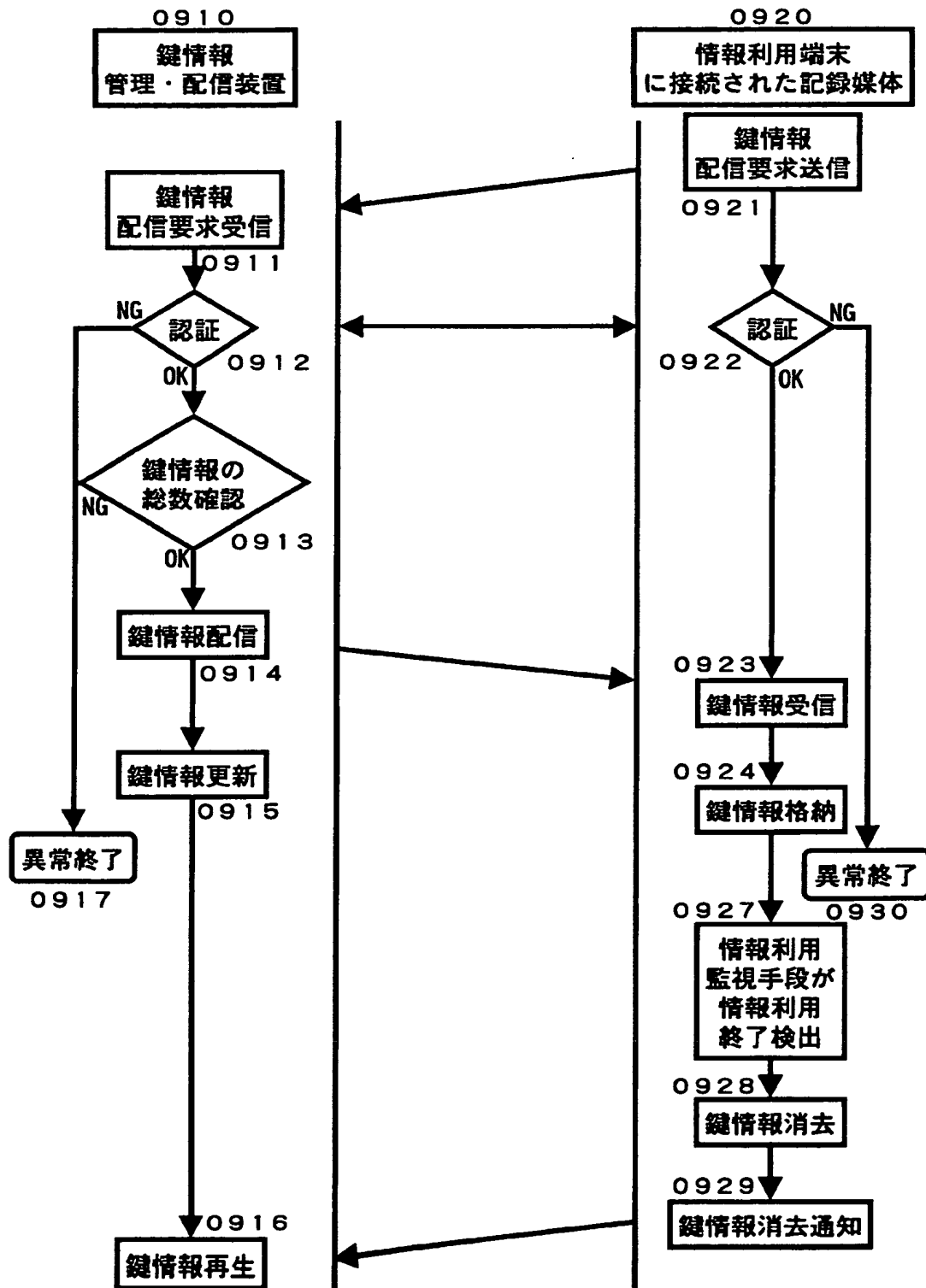
【図 7】



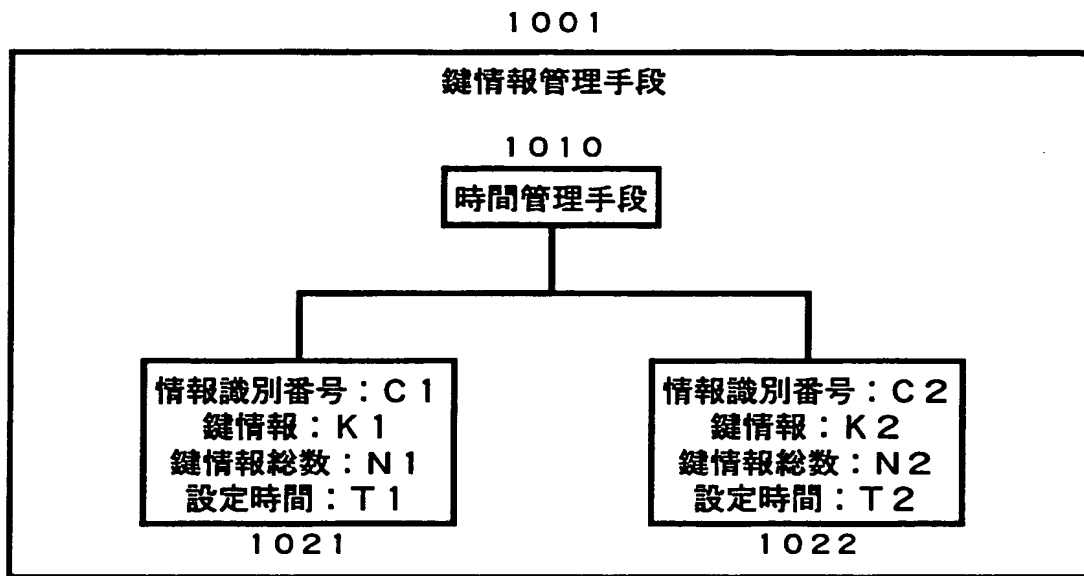
【図 8】



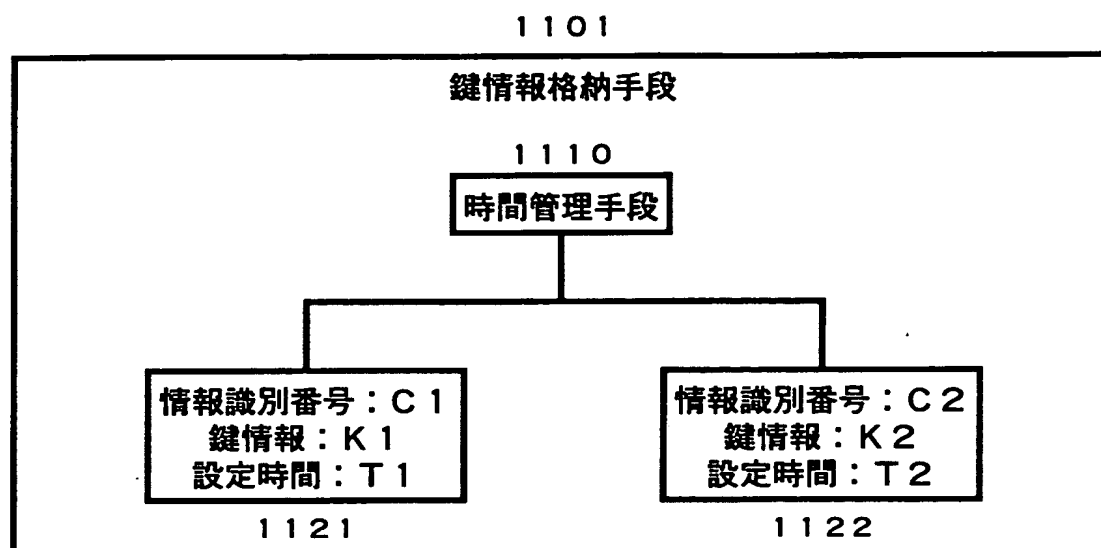
【図 9】



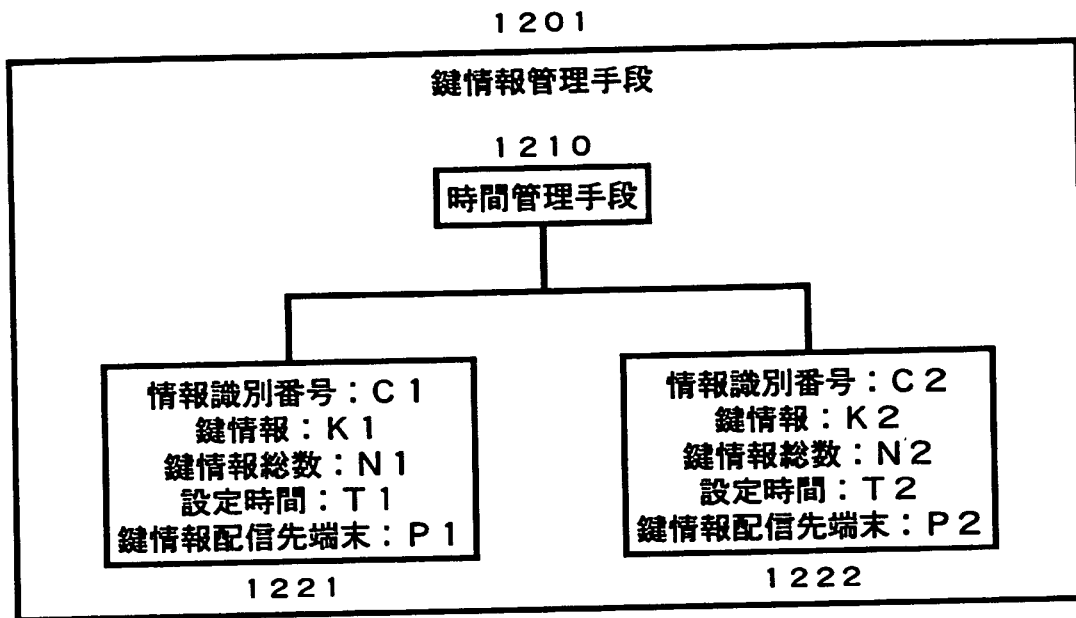
【図 1 0】



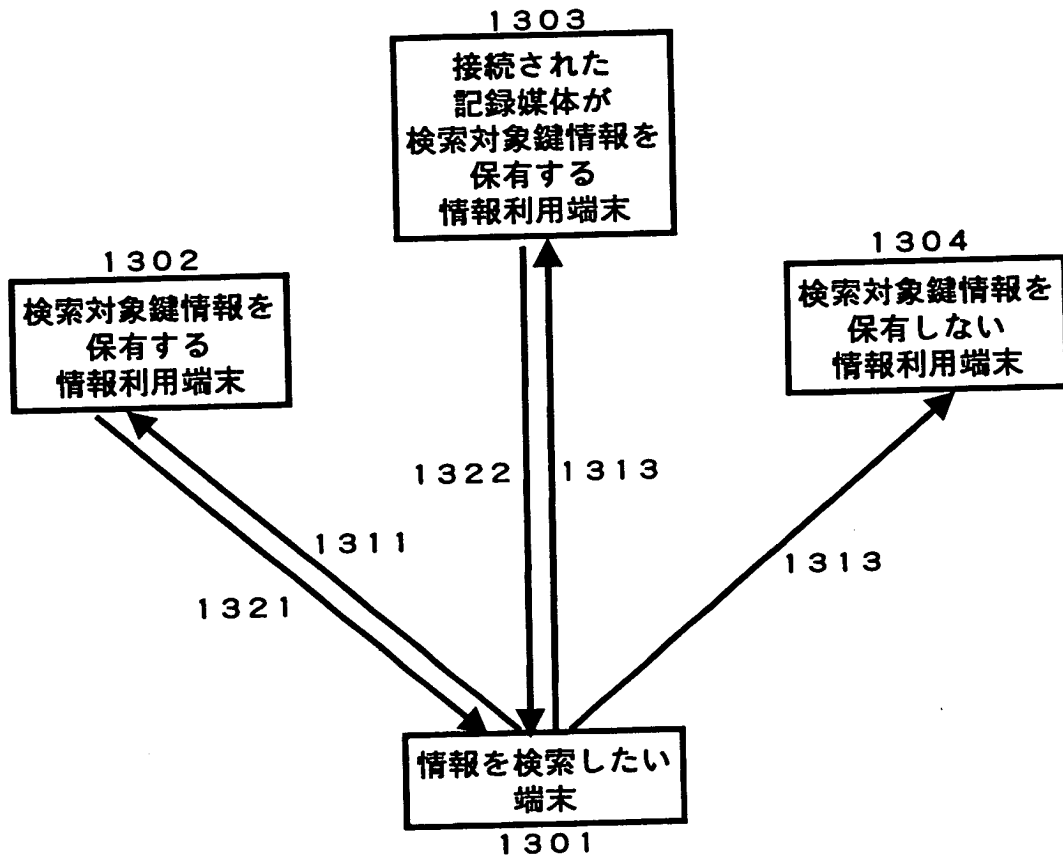
【図 1 1】



【図 12】

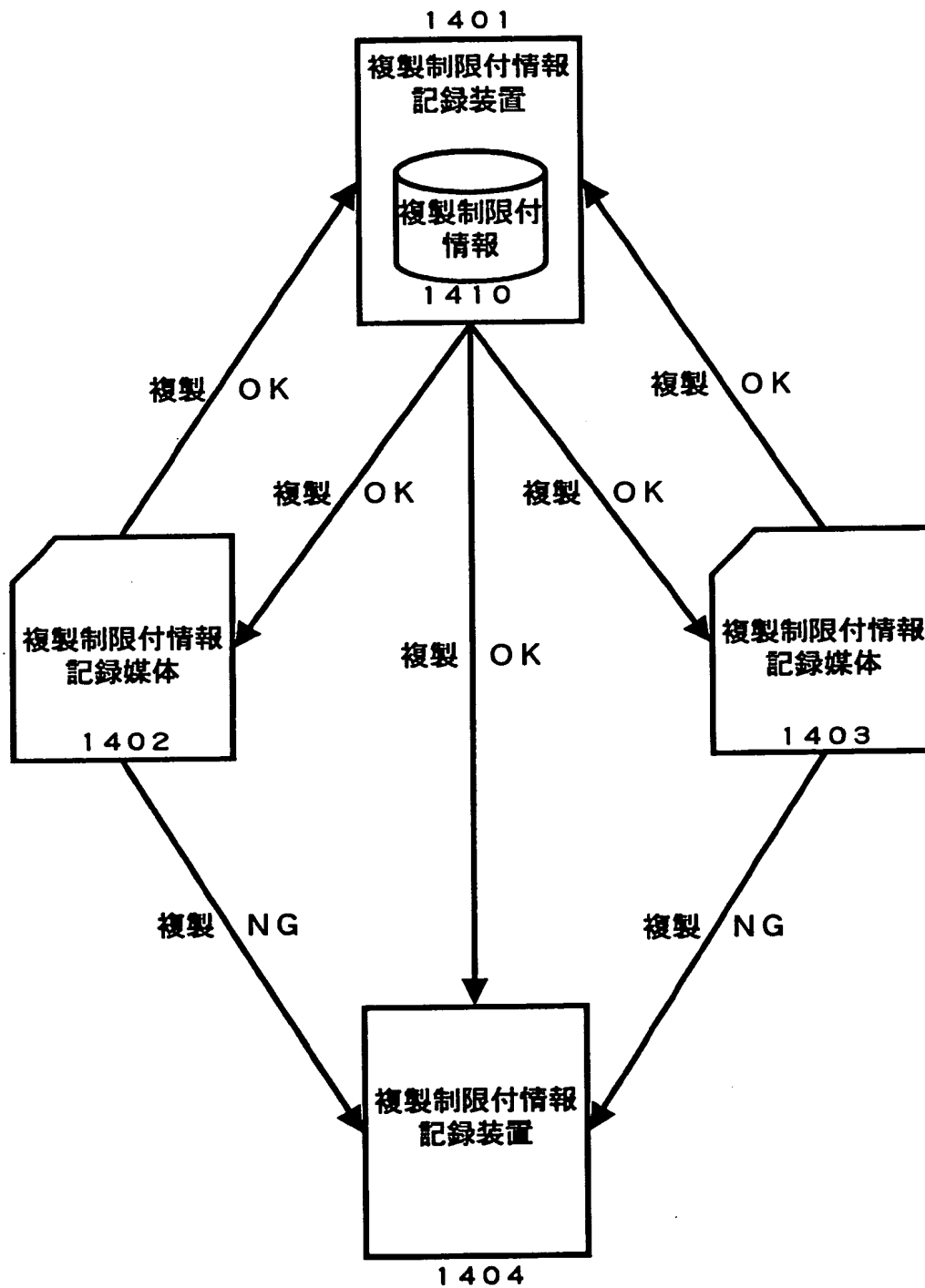


【図13】





【図14】



【書類名】 要約書

【要約】

【課題】 ネットワーク上において、ユーザの私的利用を目的とした情報の複製などを許可する一方で、情報の利用・複製に制限を設け管理することにより著作権の保護も実現する。

【解決手段】 複製・利用に制限が設けられた情報は、鍵情報とその有限な総数により利用が制限されており、鍵情報を管理するネットワークに接続された装置を用いて該情報の利用の複製・利用を管理する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社